CSWG Testing and Certification Subgroup

November 1, 2011

Assessment Guide

- CSWG management team is working on rewriting the document
- Awaiting the final changes before sending it back out for review
- Next steps
  - Review
    - CSWG
    - SGIP
  - SGIP posted document
  - SGIP CSWG F2F presentation at GridInterOp

IPRM v2.0

- Only a few comments received from the CSWG
- Schedule
  - 10/31-11/04 - SGTCC will reconcile the initial set of comments
  - 11/07 - SGTCC to release second draft for comment
  - 11/11 - Comments are due by close of business ET
  - 11/18-11/22 - SGTCC will reconcile the last set of comments
  - 12/05-12/08 - officially release IPRM v2.0 to the SGIP
- Needs to be reviewed by everyone. Sandy will keep everyone posted on the next review cycle

TOE per the PP

- The Target of Evaluation (TOE) that is described in this document is an electronic unit comprising hardware and software/firmware used for collection, storage and provision of Meter Data from one or more Meters of one or multiple commodities.

- The Gateway connects a Wide Area Network (WAN) with a Network of Devices of one or more Smart Metering devices (Local Metrological Network, LMN) and the consumer Home Area Network (HAN), which hosts Controllable Local Systems (CLS).

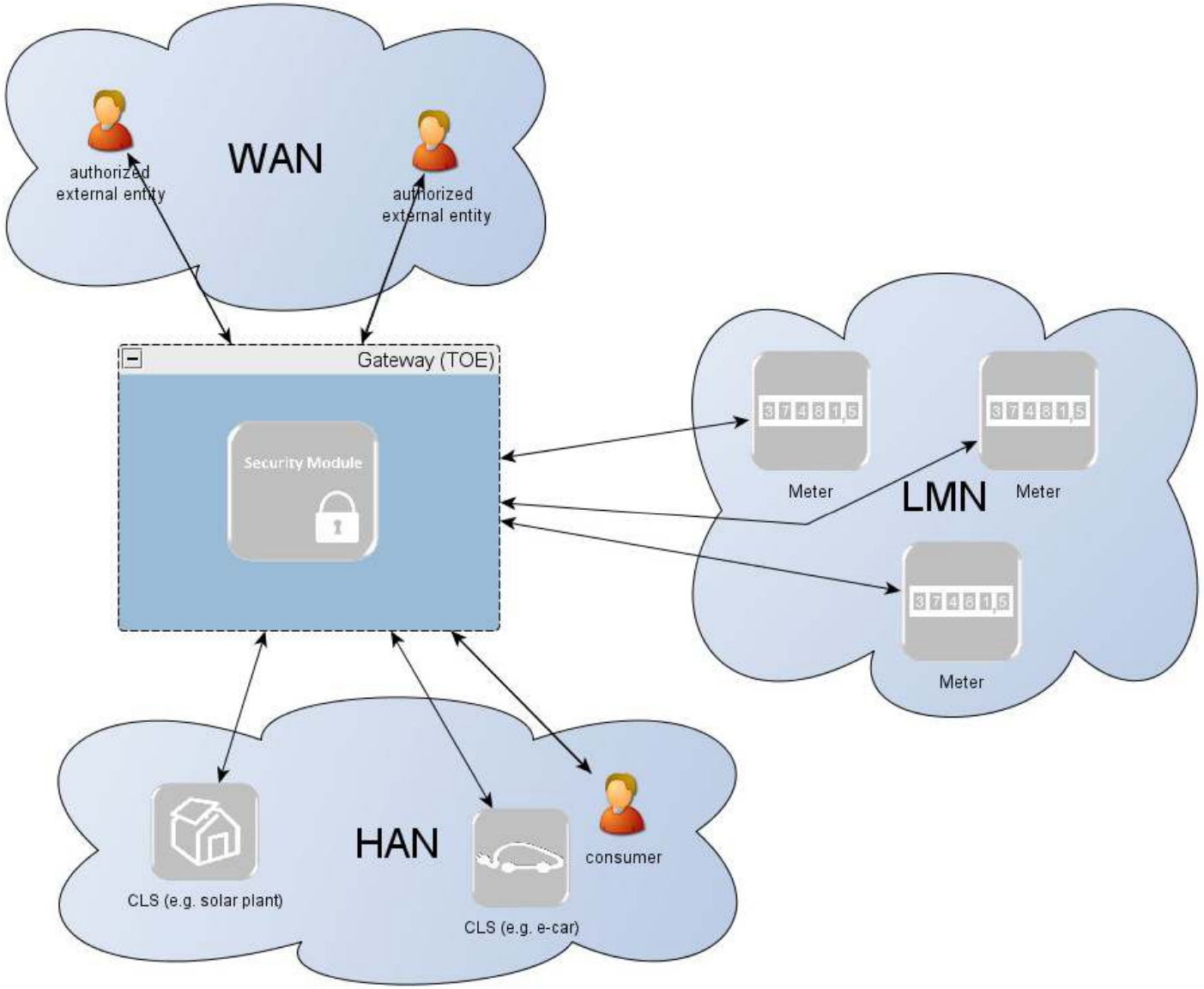
- The Smart Metering Gateway (in the following short: Gateway or TOE) may serve as the communication unit between devices of private and commercial consumers and service providers of a commodity industry (e.g. electricity, gas, water, etc.). It also collects, processes and stores Meter data and is responsible for the distribution of this data to external parties.

TOE per the PP

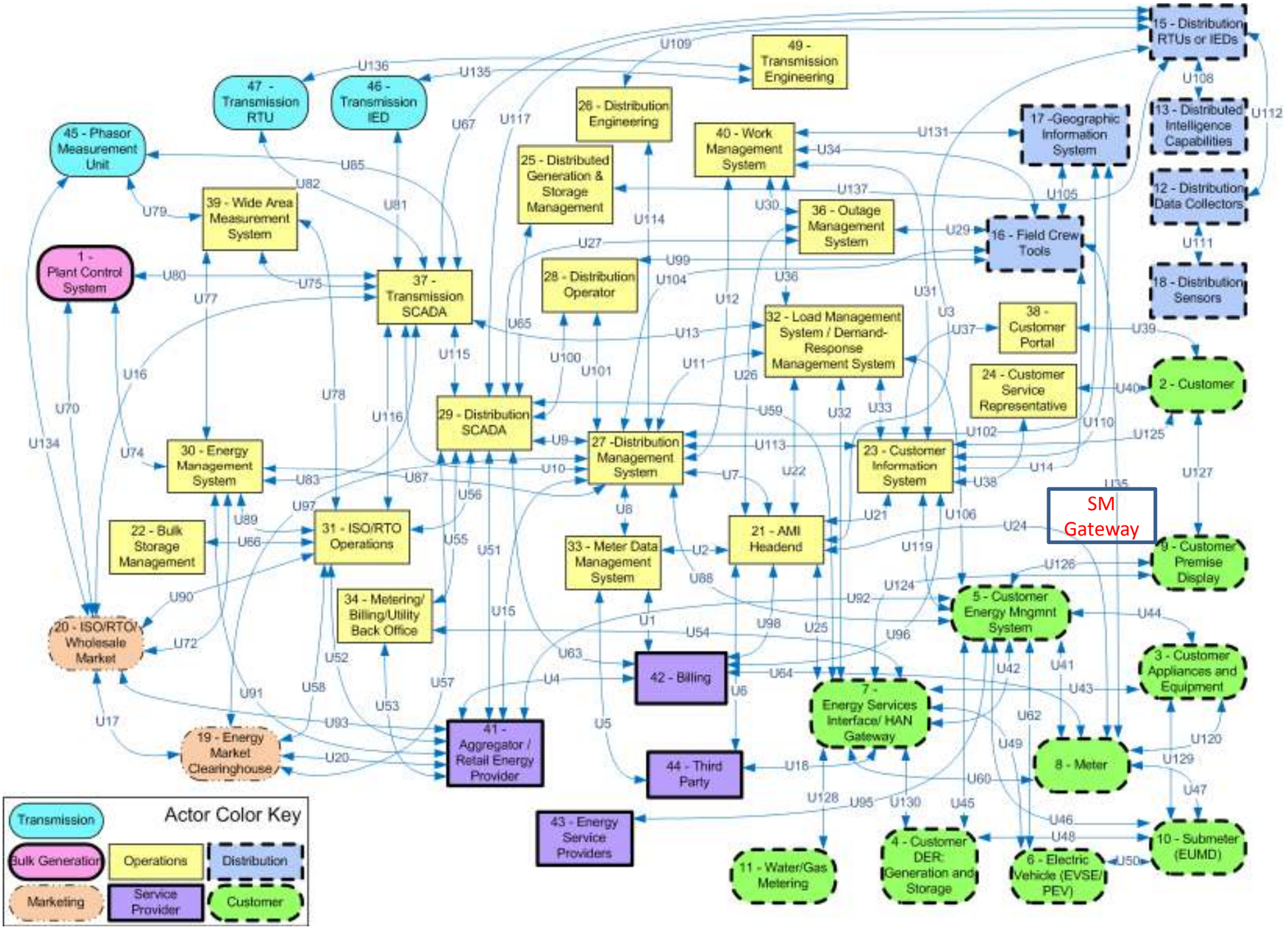
- Typically, the Gateway will be placed in the household or premises of the consumer of the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring the consumption or production of electric power, gas, water, heat etc.) and may enable access to Controllable Local Systems (e.g. power generation plants, controllable loads such as air condition and intelligent household appliances). Service providers in the context of the Gateway are the Gateway Operator, Meter Operator, Grid Operator, Commodity Supplier and others as introduced in chapter 3.1.

- The TOE has a fail-safe design that specifically ensures that any malfunction can not impact the delivery of a commodity, e.g. energy, gas or water.

TOE and its environment



Source: Protection Profile for the Gateway of a Smart Metering System, German Federal Office for Information Security


15 - Distribution RTUs or IEDs
49 - Transmission Engineering
47 - Transmission RTU
46 - Transmission IED
26 - Distribution Engineering
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
45 - Phasor Measurement Unit
40 - Work Management System
25 - Distributed Generation & Storage Management
12 - Distribution Data Collectors
39 - Wide Area Measurement System
36 - Outage Management System
16 - Field Crew Tools
1 - Plant Control System
37 - Transmission SCADA
28 - Distribution Operator
18 - Distribution Sensors
32 - Load Management System / Demand-Response Management System
38 - Customer Portal
24 - Customer Service Representative
2 - Customer
29 - Distribution SCADA
30 - Energy Management System
27 -Distribution Management System
23 - Customer Information System
SM Gateway
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
9 - Customer Premise Display
34 - Metering/ Billing/Utility Back Office
5 - Customer Energy Mngmnt System
20 - ISO/RTO/ Wholesale Market
42 - Billing
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
19 - Energy Market Clearinghouse
41 - Aggregator / Retail Energy Provider
8 - Meter
44 - Third Party
43 - Energy Service Providers
4 - Customer DER: Generation and Storage
10 - Submeter (EUMD)
11 - Water/Gas Metering
6 - Electric Vehicle (EVSE/ PEV)
Actor Color Key
Transmission
Bulk Generation
Operations
Distribution
Marketing
Service Provider
Customer

Interface into the gateway (at least)

- U18
- U24
- U25
- U32
- U35
- U37
- U38
- U39
- U40
- U41
- U42
- U43
- U45
- U46
- U49
- U54
- U59
- U60
- U62
- U64
- U88
- U92
- U95
- U106
- U125
- U126
- U127
- U128
- U130

Which maps to LICs

- 13: Interface between systems that use the AMI network
- 14: Interface between systems that use the AMI network with high availability
- 15: Interface between systems that use customer (residential, commercial, and industrial) site networks
- 16: Interface between external systems and the customer site
- 17: Interface between systems and mobile field crew laptops/equipment
- 18: Interface between metering equipment
- 22: Interface between security/network/system management consoles and all networks and systems

Which maps to NISTIR Requirements-1

- All GRC requirements
- All common technical requirements
- SG.AC-12: Session Lock
- SG.AC-13: Remote Session Termination
- SG.AC-14: Permitted Actions without Identification or Authentication
- SG.AC-15: Remote Access
- SG.IA-04: User Identification and Authentication
- SG.IA-05: Device Identification and Authentication
- SG.IA-06: Authenticator Feedback

Which maps to NISTIR Requirements-2

- SG.SC-03: Security Function Isolation
- SG.SC-05: Denial-of-Service Protection
- SG.SC-06: Resource Priority
- SG.SC-07: Boundary Protection
- SG.SC-08: Communication Integrity
- SG.SC-09: Communication Confidentiality
- SG.SC-26: Confidentiality of Information at Rest
- SG.SI-07: Software and Information Integrity

Questions from last week

Source(1st column) Destination (1st row)	WAN	LMN	HAN
WAN	- (see following list)	No connection establishment allowed	No connection establishment allowed
LMN	No connection establishment allowed	- (see following list)	No connection establishment allowed
HAN	Connection establishment is allowed to trustworthy, pre-configured endpoints and via an encrypted channel only	No connection establishment allowed	- (see following list)

Table 2: Communication flows between devices in different networks

What do we want in the NISTIR?

- Lab listing and qualifying the lab for a reference in the NISTIR and also reference the IPRM